

## **Policy on the Personal Use of Social Media by Staff**

<b>Author</b>	<b>Maggie Fraser Communications and Claims Manager</b>
<b>Lead Executive</b>	<b>Chief Executive Gordon Jamieson</b>

<b>Development of Policy</b>	<b>Reviewed</b>	<b>Policy Review date</b>	<b>Reviewers/ review team</b>
<b>August 2014</b>	<b>September 2019</b>	<b>September 2021</b>	<b>Communications and Claims Manager</b>

## Document Control

Version	Date	Latest changes made by	Status	Reason for change and reviewers
2	11/9/19	M Fraser	Draft	Updates to the original policy – all track changes.

Document Approval – Name(s) of the Individual(s) representing the Approving Committee(s)/Group(s)

Reviewer's Name	Reviewer's Role	Date
Area Partnership Forum	Comments/Consultation/Approval	31/10/19
Corporate Management Team	Consultation/Approval	10/12/19

## **1. Introduction**

- 1.1 This document sets out the NHS Western Isles Policy on the personal use of social media by staff. This policy applies to what is written/posted/streamed/shared on personal social media sites during work hours and also during periods when the employee is not at work or on a rest break.
- 1.2 NHS Western Isles recognises that an ever increasing number of employees participate in social networking sites outside of work hours. In the majority of cases this is uncomplicated and trouble-free. As an organisation, we recognize and embrace the increasing role of social media in our daily lives and across the world. The intention of this policy is not to interfere with an employee's personal life. However there are potential risks/nuisances associated with the use of social media; risks which individuals may not even be aware of.
- 1.3 There is a need to provide individuals with clear guidelines (in addition to any existing professional regulatory rules, regulations, guidelines and duties that relate to communication, conduct and the use of social media) on what is considered by NHS Western Isles to be unacceptable personal use of social media by an employee, to ensure, as far as possible, that the reputations of individuals, colleagues and the organisation are safeguarded.
- 1.4 The main principle behind this policy is that conduct on-line, and conduct face-to-face, should be judged against the same high standards of integrity and behaviour which NHS Western Isles expects of its employees. Employees should think carefully about what they post on any social media sites and **be aware that social networking websites are not secure and individual privacy settings are not sufficient to stop others seeing your content/distributing your content/printing or copying and sharing your content.** Social media platforms also frequently alter their terms of usage.

## **2. Definition of Social Media**

- 2.1 The term 'social media' is an umbrella term used to describe online technologies and practices that are used to share information, knowledge and opinions. Social media services and tools can involve a combination of technology, telecommunications and some form of online social

interaction and can use a variety of different formats, e.g. text, images, video and audio.

- 2.2 Social media, as a term and for the purposes of this policy, includes social networking (e.g. Facebook, Pinterest, Google +, Instagram and LinkedIn), blogging/microblogging applications (e.g. Twitter, Tumblr, Svbtle, Medium,, Blogger and WordPress), multimedia sharing and networking applications (e.g. YouTube, Flickr and Skype), information sharing sites (e.g. Wikipedia), forums and chat rooms (e.g. Mumsnet, dating apps, Digital Spy and iVillage), e-petitions (e.g. Change.org) and personal web pages. (This list is not exhaustive.)
- 2.3 This policy is equally applicable to the use of social media via mobile access e.g. Smartphones and Blackberrys and includes the use of applications (Apps).

### **3. Scope**

- 3.1 This policy applies to all employees of NHS Western Isles, whether full time or part-time, whether on permanent contracts, secondments, fixed-term or bank/locum/consultancy contracts. The policy also applies to NHS Western Isles volunteers and anyone on work experience or similar.
- 3.2 This policy relates to the personal use of social media, whether during work hours (not generally permitted, unless authorised for specific business purposes) or outside of work<sup>1</sup>. The policy should be used, as appropriate and necessary, in conjunction with other relevant Board policies including (but not exclusive to) the Dignity at Work Policy, the Communications Strategy, the Acceptable Use of IT Policy, the Equality and Human Rights Policy, Information Governance Policies and the Employee Conduct Policy. It should also, where appropriate, be considered in line with the Board's Standards of Behaviour, Corporate Values and Objectives and any relevant professional codes of conduct.

### **4. Roles and Responsibilities**

- 4.1 NHS Western Isles will take all reasonable steps to ensure the effective governance of this policy i.e. making sure that employees are aware of this policy and their obligations relating to personal use of social media. This will be done through the Intranet, via a Finger on the Pulse staff

<sup>1</sup> Employers are not obliged to disregard conduct simply because it occurs outside the workplace, and this also applies to the use of social media outside of work.

bulletin and inclusion in the Team Brief when the policy is launched, and managers will also be required to raise awareness of the policy through their Departmental Communications Plans and at departmental induction. If unclear, employees should seek advice from their supervisor/line manager.

### ***Responsibilities when at work***

- 4.2 All NHS Western Isles IT systems and services are provided as business tools. Employees who have authorised access to the internet at work are allowed reasonable personal use, provided it does not take place during the user's recorded working hours and only where it does not impact on other business users.
- 4.3 As a general rule, NHS Western Isles employees are not permitted access to social media sites such as Facebook and Twitter during working hours, unless authorised for specific business purposes.
- 4.4 Where employees bring their own personal mobile devices into the workplace, they must limit their use of these devices to official rest breaks, such as lunch-times. Allegations of over usage of personal mobile devices for personal reasons during core business hours will necessitate management attention.

### ***Responsibilities when not at work***

- 4.5 **All employees are singularly responsible for any information they make available online, whether this was posted during work hours, during breaks or when not at work.** The Board considers employees to be responsible and accountable for all information contained on their social media pages or blogs, even if that information originated from another source (it would be expected that inappropriate information, as defined in this policy, would be removed by the employee within a reasonable time period – i.e. once it has been identified). Employees therefore must ensure that, when engaging in social media activity, they abide by the following standards:
- 4.6 Employees must not:
  - Post, send, or promote (like, re-tweet, share, etc) any information that could potentially breach patient or organisational confidentiality; constitute harassment of an individual or group or is considered

discriminatory, threatening, intimidating or illegal; or constitute defamation of character.

- Post, send, or promote (like, re-tweet, share, etc) any information that is likely to breach NHS Western Isles or NHS Scotland policies or standards; discredit services provided by NHS Western Isles; or discredit NHS Western Isles as an employer. Any such postings will be judged in terms of the likelihood of the employee's comments causing reputational damage and the scale of any such potential damage.
- Post, send, or promote (like, re-tweet, share, etc) comments or images online which, as a healthcare professional and public servant, are likely to damage the reputation of the organisation/bring the organisation into disrepute, or damage the relationship and/or trust between the staff member and the organisation, bearing in mind the stated responsibility that all staff have for 'shaping, upholding and managing' the reputation of NHS Western Isles (as defined in the Board's Communications Strategy).
- Participate (like, re-tweet, share, etc) or offer opinions online with regard to current or rumoured legal /commercial involvement of the Board.
- Send, receive, share or post on their personal accounts images/photos of NHS Scotland patients or services users in the employee's workplace (unless shared from authorised NHS sites).
- Send, receive, share or post on their personal accounts images/photos of NHS Scotland colleagues in the workplace (unless shared from authorised NHS sites).
- Post updates and statuses on NHS Western Isles business, services, achievements and developments, on their personal social media accounts, unless it is shared from an NHS approved account, or approved in advance by the Communications Manager.
- Discuss, comment on, promote (like, re-tweet, share, etc) any matter that relates to a complaint or claim.
- Discuss, comment on, promote (like, re-tweet, share, etc) work-related issues in a manner which could cause distress to individuals, damage their own reputation or that of their employer. Any legitimate concerns

should be addressed through the appropriate Board policies e.g. NHS Western Isles Grievance Policy, Dignity at Work Policy and/or local whistle-blowing procedures.

- Use or copy any trademarks or logos belonging to the NHS and must not copy or display information or material which is subject to copyright legislation, without the express permission of the owner.
- Use their NHS e-mail address to register on a social network (unless approved for work-related purposes) or include their NHS e-mail address on a personal social media account.
- Use their NHS link (including e-mail address or social media site) to obtain private work, or to direct people to their own or another person's personal/private site.

If an employee identifies the inappropriate use of a social networking site by another employee, they have a responsibility to report this to their own line manager. Employees are advised to take screenshots of any content for this purpose. This may be used as evidence.

#### 4.7 Employees are advised to:

- Familiarise themselves with this policy, the expectation of NHS Western Isles as an employer and their individual responsibilities as an employee.
- Monitor the content of their social networking pages and blogs, ensuring they comply with the above standards. Ensure that any inappropriate information or material published on their networking pages or blogs, is removed immediately and measures put in place (where possible) to avoid any further re-occurrences (e.g. blocking certain individuals). NHS Western Isles reserves the right to contact the social media provider and request removal of materials in serious cases, including but not exclusive to cases which involve a likely risk of serious reputational damage to the employer or where there have been data protection breaches.
- Abide by professional codes of conduct (e.g. NMC, GMC, Code of Conduct for Healthcare Support Workers).
- Be aware of the Copyright 1988 Act and their individual responsibilities when posting/re-posting material (bearing in mind that copying a work protected by copyright on the web has just as serious consequences as doing so in 'real life').

- Consider not disclosing their profession and/or which organisation they work for in order to minimise any reputational risks and for their own personal safety. (N.B. this would not lessen responsibilities as an NHS Western Isles employee, and it may be the case that the individual can clearly be identified as an NHS Western Isles employee in another way – e.g. by accepting colleagues as ‘friends’ on a private account, or may be identifiable by the employer/colleagues by name/photograph and other information contained on their site – a potentially higher risk in a small community such as the Western Isles).
- Make it clear when publishing their opinions on-line, that these are their own personal views and that they do not represent the views of NHS Western Isles (if employees do disclose the name of their employer).
- Familiarise themselves with social media sites’ privacy policies, settings and guidelines and pay particular attention to any posts/comments/pages that are public and could be seen and shared by anyone.
- Give consideration to the principles of the Board’s ‘Give Respect, Get Respect’ Dignity at Work Policy (which includes guidance on ‘netiquette’).
- Check they know and trust the person when receiving online ‘friend’ requests and consider whether they wish to be associated with that person and the information and/or views that person publishes online before accepting the request.
- Consider whether they wish to be associated with information and/or views published on-line by a group or forum before accepting any request to join that group.
- If in doubt, do not ‘like’ share or comment on other content.
- Be aware that criminal sanctions can apply to the creation and dissemination of certain types of content on social media sites, just as they can elsewhere. Such content includes behaviour which:
  - Amounts to harassment and/or ‘stalking’
  - Can be classed as obscene
  - Constitutes a public order offence
  - Incites racial hatred
  - Relates to or promotes terrorism
  - Can constitute contempt of court
  - Constitutes a communication which is ‘grossly offensive’ or of an ‘indecent, obscene or menacing character’ (section 127 of the



Communications Act 2003). N.B. the offence is committed by sending the message. There is no requirement that any person sees the message or has been offended by it.

- Involves sending, or causing to be sent, a communication that is false, for the purpose of 'causing annoyance, inconvenience or needless anxiety to another'.

(The above list is not exhaustive)

(Staff should also be aware that people who pass on (e.g. re-tweet or share) messages can also be prosecuted when the original message is subject to prosecution).

## **5 Governance**

- 5.1 NHS Western Isles will not routinely actively monitor staff members' social media accounts. Notwithstanding that, employees must be aware that, if a complaint or concern is made about a posting or comment (including appropriate evidence – e.g. a screenshot), NHS Western Isles will be obliged to consider the complaint/concern and take action where it is considered that there has potentially been a breach of Board policy. NHS Western Isles is also obliged to take action, in line with the Disciplinary Policy, if any postings deemed to be in breach of this policy (as described in section 4), are brought to the attention of/reported to the organisation in the absence of a formal complaint. Staff are reminded that any information posted on social media sites has the potential to become public, regardless of privacy settings.
- 5.2 All breaches or suspected breaches of this policy should be reported to line management. These will be investigated in accordance with NHS Western Isles policy as appropriate.
- 5.3 Some breaches of this policy may be considered to be so serious that they are deemed to constitute gross misconduct. Something considered to be gross misconduct could result in employee dismissal.
- 5.4 In the most serious of cases, the individual may be considered to have committed offences under civil or criminal law. In such cases, the employer would consider police involvement.
- 5.5 Should an employee find themselves the target of complaints abuse, or bullying online they should consider removing the perpetrator(s) from their

online 'friend'/'follower'list. Most sites also have mechanisms online which can be used to block the perpetrator(s) from initiating contact and also have mechanisms for reporting abuse online.

- 5.6 Should an employee find themselves targeted online by another NHS Western Isles employee, they should take a screenshot of any postings, report the matter to their line manager and consult the NHS Western Isles Dignity at Work Policy.
- 5.7 Where it is suspected that a breach has occurred whilst using NHS IT systems, including mobile computing or removable storage media, then the NHS Western Isles IT Security Policy/ Acceptable Use of IT Policy may also require to be consulted.
- 5.8 NHS Western Isles will, where necessary and legitimate, monitor/review activity from any of its workstations/devices.

## **6 Policy Review and Monitoring**

- 6.1 This policy will be reviewed every two years, or sooner, if there is a requirement to respond to changes in technology/law/organisational structures/any other reason.